2015

Government Spying and the Comparative Legal Framework of the United States of America and the United Kingdom

Joseph Hopkins

Government Spying and the Comparative Legal Framework of the United States of America and The United Kingdom

Joseph Hopkins
Comparative Constitutional Law

"That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society."

-Samuel Warren and Louis D. Brandeis, *The Right To Privacy*

Table of Contents

Part I: Introduction

Global terrorism has been one the most pressing issues confront nations in the 21st century. The September 11th attacks had wide-ranging consequences, both foreign and domestic, for the United States and its NATO allies. The War on Terror was launched with the Invasion of Afghanistan and has expanded in to Iraq, Yemen, Somalia, and Pakistan. The recent emergence of the Islamic State of Iraq and Syria has shown that, despite some progress, military action in the Middle East is far from over. Politicians from across the spectrum in the United States vowed to prevent an attack like September 11th from ever happening again. The main weapon in preventing such attacks has been the acquisition of electronic surveillance data by the National Security Agency, authorized by the Foreign Intelligence Surveillance Act.

The United Kingdom of Great Britain has been one of the United States' most steadfast allies in the War on Terror. While not directly affected by the September 11th attack, the United Kingdom is not a stranger to the threats posed by terrorism, as the London bombing of July 2005 and conflicts with various iterations of the Irish Republican Army have shown. The Regulation of Investigatory Powers Act 2000 authorized the Government Communications Headquarters to collect electronic data on the basis of national security concerns.

For over a decade, most Americans and Britons were unaware of just how expansive and invasive their government's spying programs were. Due to the courage of Edward Snowden, the dark secrets of the most powerful government agencies were brought into the light in June of 2013. Snowden, a former NSA contractor, leaked numerous documents exposing how the NSA had been abusing its power by collecting electronic data on millions of Americans with no connection to terrorism. In addition, Snowden revealed how the NSA's British counterpart, the

Government Communications Headquarters, had constructed a similarly expansive program that collected data on law-abiding citizens.

Edward Snowden's motivations and goals were questioned by the media after the leaks were published. Snowden is a heroic patriot to some and a traitor who damaged national security to others. When ask by journalist Glenn Greenwald why he acted, Snowden explained:

> "I really want the focus to be on these documents and the debate which I hope this will trigger among citizens around the globe about what kind of world we want to live in. My sole motive is to inform the public as to that which is done in their name and that which is done against them."[1]

Whether or not one takes Snowden at his word, a debate has certainly been triggered about the legality of the methods used by government intelligence agencies and how ordinary citizens should go about changing the system.

This paper aims to discuss the legal framework and resulting surveillance practices in the United States and United Kingdom and analyze how each model affects the potential for redress. Part II examines the Fourth and Fourteenth Amendments and the growth of right of privacy jurisprudence in the civil and criminal contexts during the 1960's. Part II then discusses the legal framework of the Foreign Intelligence Surveillance Act of 1978 and the subsequent statutory developments in the aftermath of the September 11 attacks, particularly the FISA Amendments of 2008.

Part III begins by tracing the United Kingdom's development of privacy in the civil context via common law and the Data Protection Act 1998 and through the Police and Criminal Evidence Act of 1984 in the criminal context. As the United Kingdom is part of the European Union, this section also covers the interrelatedness of European Convention on Human Rights

---

[1] Glenn Greenwald, Ewen MacAskill, and Laura Poitras, "Edward Snowden: the whistleblower behind the NSA surveillance revelations," The Guardian, June 11, 2013, http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

and the Human Rights Act. Lastly, Part III discusses the Regulation of Investigatory Powers Act and the broad power that it gave the government to collect data on its own citizens.

Part IV traces the wide-ranging collection of data by various spying programs designed by the National Security Agency and their exposure by Edward Snowden in June 2013. Part IV discusses the collection programs anchored by the NSA's British counterpart, the Government Communications Headquarters, which were revealed by Snowden as well. This section also discusses the joint efforts by the U.S. and British governments to share data that they both collect.

Part V analyzes the protections afforded to citizens on the basis of the United States and Great Britain's constitutional framework. This section compares the avenues from redress inherent in the United States Constitution through the concept of judicial review versus the long-rooted tradition of parliamentary sovereignty in the United Kingdom.

Part II: The United States of America

A. *Constitutional and Judicial Origins of the Right to Privacy*

The right to privacy is not found explicitly in the Constitution of the United States of America, which functions are the supreme law of the land. Instead, the right to privacy was first recognized in *Griswold v. Connecticut*, where the Supreme Court held a law banning the use of contraceptives as unconstitutional.[2] Writing for the majority, Justice William Douglas espoused his "penumbra" theory of constitutional protections from which zones of privacy are created through an interworking of the various guarantees listed in the Bill of Rights, such as the First Amendment's freedom of association, the Third Amendment's prohibition against the quartering of soldiers, the Fourth Amendment's right against unreasonable searches and seizures, the Fifth Amendment's Self-Incrimination Clause, and the Ninth Amendment's addressing of

[2] *Griswold v. Connecticut*, 381 U.S. 479 (1965)

unenumerated rights.[3] However, the right to privacy has more often been seen as an extension of the Fourteenth Amendment's Due Process Clause, which declares that no state shall "deprive any person of life, liberty, or property, without due process of law." The Due Process Clause approach was endorsed by Justices Harlan, White, Goldberg, Warren, and White in *Griswold.* The Due Process Clause and the concept of sexual privacy that follows has been the justification for striking down bans on abortion in *Roe v. Wade* and laws criminalizing sodomy in *Lawrence v. Texas.*[4]

The Fourth Amendment governs the right of privacy in the criminal context. The Fourth Amendment states that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The basic framework for when the government needs a search warrant is governed by *Katz v. United States.* In *Katz*, the court held that "Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth" and thus constituted a "search and seizure" within the meaning of the Fourth Amendment."[5] Justice John Harlan II's concurrence created so-called *Katz* Test to determine whether the defendant has a reasonable expectation of privacy from a search which asks "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[6]

---

[3] *Id.* at 484
[4] *Roe v. Wade*, 410 U.S. 113, 153 (1973); *Lawrence v. Texas*, 539 U.S. 558, 565 (2003)
[5] *Katz v. United States*, 389 U.S. 347, 353 (1967)
[6] *Id.*

However, subsequent Supreme Court decisions have built upon the premise that 4th Amendment does not provide a blanket right to privacy. For example, *Arizona v. Hicks* stated that that only probable cause is required to invoke the "plain view" doctrine as it applies to seizures.[7] Similarly, in *Chimel v. California*, the Supreme Court upheld the constitutionality of a search incident to arrest, writing that "it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape."[8]

The Supreme Court has examined the relationship between the warrant requirement and domestic national security concerns in *United States v. United States Dist. Court.*[9] The government charged the three defendants with conspiracy to bomb a CIA office in Ann Arbor, Michigan. The main piece of evidence was electronic surveillance obtained without a warrant via the Omnibus Crime Control and Safe Streets Act 1968. Writing for a unanimous 8-0 majority, Justice Powell held that in cases of domestic national security, electronic surveillance "must be exercised in a manner compatible with the Fourth Amendment" by having proper judicial approval.[10] However, the Court was careful to use limiting language, noting that Congress may "involve different policy and practical considerations from the surveillance of ordinary crime" when articulating a probable cause standard or might create a specifically designated court to approve electronic surveillance warrants.[11] More importantly, the Court noted that the opinion did not address "issues which may be involved with respect to activities of foreign powers or their agents."[12]

---

[7] Arizona v. Hicks, 480 U.S. 321, 326-328 (1987)
[8] Chimel v. California, 395 U.S. 752, 763 (1969)
[9] United States v. United States Dist. Court, 407 U.S. 297 (1972)
[10] *Id.* at 320
[11] Id. at 323.
[12] Id. at 322

B. *The Foreign Intelligence Surveillance Act of 1978 and subsequent 2008 Amendments*

The original legislative framework for the National Security Agency's spying programs is the Foreign Intelligence Surveillance Act of 1978 (hereafter referred to as FISA). The Church Committee hearings of 1975-76 revealed that the FBI, CIA, and NSA had been monitoring the electronic communications of American citizens for three decades without any warrants. Targets of the spying were mainly anti-Vietnam activists and included prominent figures for different areas of life such as boxer Muhammad Ali, journalist Tom Wicker, satirist Art Buchwald, civil rights leader Martin Luther King, Jr., and even Senator Frank Church himself.[13]

In response to these revelations, Congress passed the Foreign Intelligence Surveillance Act with the purpose of providing protections for American citizens without impeding the collection of foreign intelligence information vital to national security.[14] FISA gives the President, through the Attorney General, the power to authorize electronic surveillance without a court order to collect foreign intelligence information for up to a year as long as the surveillance is solely directed at communication between foreign powers, there no substantial likelihood that communications of a U.S. person will be acquired, and that the proper minimization procedures are in place to limit the unintentional acquisition of communications by U.S. persons.[15] The

---

[13] Ed Pilkington, "Declassified NSA files show agency spied on Muhammad Ali and MLK," The Guardian, September 26, 2013, http://www.theguardian.com/world/2013/sep/26/nsa-surveillance-anti-vietnam-muhammad-ali-mlk.

[14] Foreign intelligence information has a very broad scope which is defined under 50 U.S. §1801(e) as: (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States.

[15] 50 U.S. §1802(a)(1)

warrantless surveillance power is limited in scope because it does not apply to individuals in foreign nations based on the definition of foreign power.[16]

In order to conduct surveillance on persons, the government must meet a number of criteria under 50 U.S. §1804(a) with the major requirements being that "the target of the electronic surveillance is a foreign power or an agent of a foreign power" and "the significant purpose of the surveillance is to obtain foreign intelligence information."[17] "Agent of a foreign power" serves as an important definition crafted to limit the scope of who can be targeted. Any person not a U.S. citizen is an agent of a foreign power if one acts in the U.S. as an officer of a foreign power, engages, conspires or engages in clandestine intelligence activities contrary to U.S. interest, or engages in terrorism.[18] A U.S. citizen, or anyone else, may also be considered an "agent of a foreign power" if one knowingly engages in clandestine activities for a foreign power in violation of criminal statutes, "knowingly engages in sabotage or international terrorism on behalf of a foreign power", or "knowingly enters the United States under or later assumes a false or fraudulent identity for or on behalf of a foreign power."[19]

FISA also requires that minimization procedures are in place. Minimization procedures are defined as "specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to

---

[16] Foreign power for the purposes of warrantless surveillance under 50 U.S. §1802(a)(1) is limited to: (1) a foreign government or any component thereof, whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons;(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments. 50 U.S. §1801(a)(1)-(3). It does not apply to "a group engaged in international terrorism or activities in preparation therefor" as defined under 50 U.S. §1801(a)(4).

[17] *Id.* In addition, each application should include a description of the target, type of information sought, and the format in which the information is kept, and that the proper minimization procedures are in place.

[18] 50 U.S. §1801(b)

[19] Id.

minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons."[20]

FISA also created the United States Foreign Intelligence Surveillance Court (hereafter referred to as FISC) to review warrant applications. The current FISC is comprised of eleven judges, each of whom is appointed by the Chief Justice for a single, non-renewable term that may last up to seven years.[21] The FISC is tasked with reviewing whether or not the government has shown probable cause that the target is an agent of a foreign power, that the object searched is being used by said agent, and that the minimization procedures are in place.[22]

After the September 11 attacks, the scope of electronic surveillance increased the dramatically. A number of statutes were passed and procedures created that expanded the role of government surveillance due to the perceived threat of terrorism, including the PATRIOT Act, President's Surveillance Program, and Protect America Act of 2007. Many of these acts were incorporated into the FISA Amendments Act of 2008 (hereafter referred to as FAA) which has been cited as the overarching authority for the NSA's electronic surveillance programs.

The FAA makes several substantial changes to the FISA framework that essentially allows the government to acquire a mass surveillance warrant with alarming ease. The law allows the Attorney General and the Director of National Intelligence for a period of up to 1 year to target "persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[23] The new warrantless surveillance language is critical to creation of the NSA's programs. As opposed to the much more restrictive definition of "agent of a foreign power," the alteration means that any foreign person may be targeted, greatly expanding the

---

[20] 50 U.S. §1801(h)
[21] 50 U.S. §1803
[22] 50 U.S. §1805
[23] 50 U.S.C §1881a(a), better known to the public as §702(a)

collection ability of the NSA. The FAA states that the government should not intentionally target U.S. citizen without a warrant. However, provided that one person is a foreigner, the NSA may collect the data, even if one of its senders or recipients is an American.[24]

To obtain such an authorization, the government must only show to the FISC that certification procedures are in place to "ensure that an acquisition...is limited to targeting persons reasonably believed to be located outside the United States," "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States," "a significant purpose of the acquisition is to obtain foreign intelligence information," and are "consistent with the requirements of the fourth amendment."[25] In addition, the government no longer has to "identify the specific facilities, places, premises, or property" that it will be monitoring.[26]

The FISC has a very limited role in reviewing government actions taken under the FAA. The FISC only need to find that the certification has all the required elements; the target is reasonably believed to be located outside the U.S. and that the proper minimization procedures are in place.[27] Even if the FISC does find that the certification to be deficient, the government may continue its surveillance during the appeal process.[28]

---

[24] 50 U.S.C §1881a(b). In full, 50 U.S.C §1881a(b) states that the information gathered under 50 U.S.C §1881a(a) may not: (1) "intentionally target any person known at the time of acquisition to be located in the United States"; (2) "intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;" (3) intentionally target a United States person reasonably believed to be located outside the United States;" (4) "intentionally acquire any communication as to which the *sender and all intended recipients* are known at the time of the acquisition to be located in the United States." (emphasis added)

[25] 50 U.S.C §1881a(g)

[26] 50 U.S.C §1881a(g).

[27] 50 U.S.C §1881a(i)

[28] *Id.*

Part III: The United Kingdom of Great Britain

A. Acts of Parliament and the European Union

The United Kingdom of Great Britain is a constitutional monarchy that does not have a written constitution in the mold of the United States of America. Instead, British law is rooted in the idea of parliamentary sovereignty, which is holds that Parliament is "the supreme legal authority in the [United Kingdom], which can create or end any law."[29] Since Acts of Parliament function as the supreme law of the land, they are not subject to domestic judicial review. Parliament has the duty to monitor its acts and their effects on the citizenry, which is done through questioning the prime minister, debates, and committees.[30]

However, the authority of Parliament is not absolute, and various courts play a vital role in British governance. As a general matter, the United Kingdom is subject to legislation enacted by the European Union and bound by decisions from the European courts. The European Communities Act 1972 states that "all such rights, powers, liabilities, obligations and restrictions from time to time created or arising by or under the Treaties were to be given legal effect or used in the United Kingdom shall be recognised and available in law, and be enforced, allowed and followed accordingly."[31] The *Factortame* case held that European Union Community legislation overrides British law to the extent to which "a national measure in clear terms will, if applied, automatically deprive that party of the rights" under a conflicting Community law.[32]

---

[29] *See* http://www.parliament.uk/about/how/sovereignty/
[30] *See* http://www.parliament.uk/about/how/role/scrutiny/
[31] European Communities Act 1972 Section 2(1); *URL:* http://www.legislation.gov.uk/ukpga/1972/68/enacted
[32] *R v Secretary of State for Transport, ex p. Factortame Ltd* (No. 1) [1989] UKHL 1 (18 May 1989); *URL:* http://www.bailii.org/uk/cases/UKHL/1989/1.html

B. *Growth of British Privacy Law in the 20th Century*

Under British common law, no general right of privacy exists. Instead, there are several tort claims that one can bring that include trespass, nuisance, defamation, breach of confidence, and malicious falsehood.[33] However, recent statutory developments, influenced by sources from the European Union, have modernized British privacy law.

The Data Protection Act 1998 is a complex law that regulates how a data controller can process personal data.[34] A "data controller" is any person or organization and "processing" means obtaining, recording or holding of said data. The act differentiates among certain types of data and what can be done legally with such data. The act defines "personal data" as any data that can be used to identify a living individual.[35] This sort of data is governed by eight principles listed in Schedule I that summate that data should be processed within the scope of the purpose that it was collected for and that reasonable technological measures should be in place to prevent others from accessing it.[36] Further, the act defines "sensitive person data" as data that contain information on one's race, political opinions, religion, health, sexual life, or criminal history.[37] This data is governed much more strictly and should only be processed with one's consent or in accordance with the law. However, the act carves out certain exceptions for when data can be released without permission, such as for national security, law enforcement, and taxation purposes or for journalistic, literary, or artistic matters that are of public interest.[38]

The British Parliament has also taken steps to incorporate European Union law domestically. The Human Right Act 1998 aimed to further incorporate the European Convention

---

[33] Wainright v. Home Office [2003] UKHL 5
[34] Data Protection Act, 1998, c. 29, § 1
[35] *Id.*
[36] 1998 c. 29, sch. I
[37] 1998 c. 29, § 2
[38] 1998 c. 29 §28-37

on Human Rights (ECHR) into British law. Among the various rights listed in ECHR, Article 8 states "everyone has the right to respect for his private and family life, his home and his correspondence" subject to certain instances where it is necessary for "national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[39]

The Human Rights Act creates a limited form of judicial review of Acts of Parliament by allowing judges to declare laws incompatible.[40] When reviewing an act, the court should first try to construe the statute in a way that makes the act comport with European law. If the court cannot, the court will declare the law incompatible. However, a declaration of incompatibility "does not affect the validity, continuing operation or enforcement of the provision."[41] A minister of the Crown may then take a remedial measure to amend the legislation, but parliamentary approval will be needed to make the change permanent.[42]

British law implicitly recognizes the right to privacy in the criminal context. The Police and Criminal Evidence Act 1984 spells out the procedures law enforcement must take when searching a suspect's home or person. In general, a constable must show that there are reasonable grounds for believing "(a) that an indictable offence has been committed; (b) that there is material on premises which is likely to be of substantial value (whether by itself or together with other material) to the investigation of the offence; and (c) that the material is likely to be relevant evidence."[43] The act does provide exceptions if the item is privileged legal information, journalistic material held in confidence, a business documents, or documents related to holding

---

[39] *See* http://conventions.coe.int/treaty/en/Treaties/Html/005.htm
[40] Human Rights Act, 1998, ch. 42, § 3
[41] Human Rights Act, 1998, ch. 42, § 4
[42] Human Rights Act, 1998, ch. 42, § 10; Human Rights Act, 1998, ch. 42, sch. 2
[43] Police and Criminal Evidence Act, 1984, c. 60, § 8

public office.[44] Incident to an arrest, a constable may enter and search any premises occupied or controlled by a person if he has reasonable grounds for believing evidence related to the offense or similar offense is present.[45]

C. *Privacy and the Regulation of Investigatory Powers Act 2000*

The Regulation of Investigatory Powers Act 2000 (hereafter RIPA) is the governing law that regulates the interception of communications and the acquisition of data in the United Kingdom.[46] The act creates five types of surveillance governed in different ways, the most important of which are "interceptions of communications" and "communications data."[47] Communications data is defined as any postal or telecommunications system that identifies the person, apparatus, or location from which the communication is transmitted.[48] Importantly, this definition excludes access to the content of the data itself. This sort of metadata collection can be done under almost any pretense provided that it is deemed necessary for national security, crime, economic well-being, public safety, public health, taxes, and preventing injury or death.[49] Regarding who can order such surveillance, the act differentiates by rank in the relevant public authorities as prescribe by the Secretary of State.[50] RIPA also has provisions for the acquisition of communications data from foreign agencies. The act states that "data can only be disclosed when the appropriate authority is satisfied that it is in the public interest to do so and all relevant conditions imposed by domestic legislation have been fulfilled."[51]

---

[44] Police and Criminal Evidence Act, 1984, c. 60, § 10-14
[45] Police and Criminal Evidence Act, 1984, c. 60, § 18
[46] Regulation of Investigatory Powers Act, 200, c. 23, Introduction
[47] The other three are "Intrusive Surveillance" (surveillance in a premise or vehicle with a listening or video device), "Directed Surveillance" (surveillance in a public place to monitor a specific target) and "Covert Human Intelligence" (undercover agents). Regulation of Investigatory Powers Act, 2000, c. 23, § 26
[48] Regulation of Investigatory Powers Act, 2000, c. 23, § 21
[49] Regulation of Investigatory Powers Act, 2000, c. 23, § 22
[50] Regulation of Investigatory Powers Act, 2000, c. 23, § 25
[51] Regulation of Investigatory Powers Act, 2000, c. 23, § 171

The "interception of communications" provision allows the government to collect vast amounts of internet and phone information, including the content of such data.[52] Before issuing a warrant, the government must first show the interception is in the interest of national security, for the purpose of preventing or detecting serious crime, or for the purpose of safeguarding economic well-being.[53] Second, the government must believe that "the conduct authorised by the warrant is proportionate to what is sought to be achieved." The warrant itself only needs to list the person and places that is the subject of the interception.[54] RIPA also authorizes warrants, called 8(4) warrants, for the mass collection of external communications that originate or terminate outside the United Kingdom as long as the collection is for the aforementioned interests.[55] For both types of warrants, the data provider is required to provide whatever information it has on the target for further the goals of the warrant.[56]

Part IV: Edward Snowden and the June 2013 global surveillance leaks

A. The NSA and the PRISM Program

In early June 2013, *The Guardian* and *The Washington Post* began to publish stories exposing government spying programs instituted by the National Security Agency.[57] The first leaked document showed that on April 25, 2013, the FISC had ordered Verizon Wireless, the largest telecommunications company in the U.S., to supply the NSA with telephone metadata between person in the U.S. and wholly within the United States. The information to be turned over included identifying information such as the phone numbers, international mobile subscriber identity number, international mobile station equipment number, times of the calls,

---

[52] Regulation of Investigatory Powers Act, 2000, c. 23, § 2
[53] Regulation of Investigatory Powers Act, 2000, c. 23, § 3
[54] Regulation of Investigatory Powers Act, 2000, c. 23, § 8
[55] *Id.*
[56] Regulation of Investigatory Powers Act, 2000, c. 23, § 11
[57] For Glenn Greenwald's account of his experience with Edward Snowden, *see* Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (New York: Metropolitan Books, 2014).

and duration of the calls. However, the order states that substantive content, name, address, or financial information should not be included.[58]

The second major disclosure by the *Guardian* revealed the existence of the PRISM program. The PRISM program collects, depending on the service or company that is providing the NSA with data, information on a multitude of items including e-mails, videos, photos, files transfer, and network activity. Companies that PRISM is allowed to directly collect data from are the largest in the world, including Microsoft, Yahoo, Google, Facebook, YouTube, Skype, and Apple. The leaked NSA slides stated that the PRISM program is the number one source for all the data collected by the NSA.[59] In addition, the PRISM Program works in conjunction with other NSA initiatives, codenamed BLARNEY, OAKSTAR, FAIRVIEW and STORMBREW, that collect data directly fiber cables and other electronic infrastructure.[60]

There is some debate whether or not the NSA has been accessing the content of data being collected. James Clapper, the Director of National Intelligence, has repeatedly stated that the NSA does not listen to the content of phone data or view the content of electronic data.[61] However, this statement contradicts the vast majority of articles written about the NSA's surveillance practices which state that PRISM program does just that.[62]

---

[58] For the text of the order, see http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order.
[59] Glenn Greenwald and Ewen MacAskill, "NSA Prism program taps in to user data of Apple, Google and others," The Guardian, June 7, 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.
[60] Craig Timberg and Barton Gellman, "NSA paying U.S. companies for access to communications networks," The Washington Post, August 21, 2013, http://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html.
[61] Dan Roberts, Spencer Ackerman, and Tania Branigan, "Clapper admits secret NSA surveillance program to access user data," The Guardian, June 7, 2013, http://www.theguardian.com/world/2013/jun/07/clapper-secret-nsa-surveillance-prism.
[62] Charlie Savage, "N.S.A. Said to Search Content of Messages to and From U.S.," The New York Times, August 8, 2013, http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?page wanted=all&_r=1&.

After the data is collected, it is stored in databases: MARINA for internet data and MAINWAY for telephony data.[63] Once stored, the NSA has extremely broad powers to search through data pertaining to any target through the XKeyscore system, which has approximately 150 sites and 700 servers around the world.[64] XKeyscore indexes everything from emails, files, internet traffic, and phone numbers.[65] According to Snowden, the data can be searched at will with no supervision.[66]

B. The GCHQ and Tempora Program

The Snowden leaks also shed light on the GCHQ's role in global surveillance.[67] The GCHQ has developed a similar program to PRISM, codenamed Tempora, which has two components dubbed "Mastering the Internet" and "Global Telecoms Exploitation." The "Mastering the Internet" initiative has been able to collect massive amounts of data by directly tapping into internet cable lines. The data collected is then stored for 30 days.[68] According to the *Guardian*, the information included "recordings of phone calls, the content of email messages, entries on Facebook and the history of any internet user's access to websites."[69] The Guardian further noted that documents they examined showed that the "GCHQ was handling 600 [million] 'telephone events' each day, had tapped more than 200 fibre-optic cables and was able to process

---

[63] Kevin Drum, "Washington Post Provides New History of NSA Surveillance Programs," Mother Jones, July 15, 2013, http://www.motherjones.com/kevin-drum/2013/06/washington-post-provides-new-history-nsa-surveillance-programs.
[64] *See* http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation
[65] *Id.*
[66] Glenn Greenwald, "XKeyscore: NSA tool collects 'nearly everything a user does on the internet,'" The Guardian, July 31, 2013, http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.
[67] While slides prepared by the NSA and FISC court orders were made public, documents relating to the Tempora program were generally not released. Therefore, information on the Tempora program is not as robust and the access and review reported by the *Guardian* and *Washington Post* will be assumed to be correct.
[68] Ewen MacAskill et al., "GCHQ taps fibre-optic cables for secret access to world's communications," The Guardian, June 21, 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.
[69] *Id.*

data from at least 46 of them."[70] Another program, named Optic Nerve, indiscriminately collected millions of images from Yahoo webcam chats, many of the images being of a sexually explicit nature.[71]

The GCHQ and the NSA have also closely cooperated to share data via the MUSCULAR program. Leaked documents revealed that swaths of account information from Google and Yahoo were taken from fiber-optic cable in Britain and transferred to the NSA's headquarters in Fort Meade, Maryland.[72] The documents allege that on January 9, 2013, the NSA was given over 180 million new records which included the content of those records.[73] Moreover, the documents also allege that the United States was sharing data it had collected on British citizens with the GCHQ.

Part V: Analysis

A. National Security versus Privacy Rights

The struggle between national security and privacy rights is directly connected to the remedies that each constitutional system provides. There are two competing mindsets in the debate on the role of electronic surveillance in society. The first is that electronic surveillance is necessary to protect the country from terrorism and whatever potential privacy violations occur are either minor or outweighed by the threat posed by terrorism. However, critics note the ineffectiveness of program such as PRISM, citing the NSA's failure to prevent the 2013 Boston Marathon Bombing, despite the perpetrators' significant digital footprint that indicated

---

[70] *Id.*
[71] Spencer Ackerman and James Ball, "Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ," The Guardian, February 28, 2014, http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.
[72] Barton Gellman and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," The Washington Post, October 30, 2013, http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.
[73] *Id.*

radicalization.[74] The NSA has attempted to provide examples of plots thwarted, but no definitive example has yet to be produced.[75]

The second mindset is that the invasions of privacy are much more significant than the government cares to admit and that law abiding citizens should simply have to right to conduct their activities in peace. In addition, there is an underlying fear that the government may use the vast information that is has to crack down on political dissent and stifle journalism. Given the NSA's past history of spying on anti-Vietnam protesters, this scenario is not too far-fetched. About a month before the Snowden revelations, the Justice Department had come under fire for secretly collecting phone records on as many as one hundred journalists and editors for *The Associated Press*.[76] In particular, Attorney General Holder was criticized for subpoenaing the e-mail of a Fox News reporter, James Rosen, by charging him as a co-conspirator of Stephen Jin-Woo Kim, who was sentenced to 13 months in prison for disclosing national defense information. In addition, the British government detained and interrogated David Miranda, Glenn Greenwald's domestic partner, for nine hours in what Greenwald described as an episode that was "obviously designed to send a message of intimidation to those of us working journalistically on reporting on the NSA and its British counterpart, the GCHQ."[77]

B. The Importance of Constitutional Framework

The framework provided by each nation's constitution will be vital in determining what avenues of redress are available when one's rights are being violated. The framers of the

---

[74] Michael Daly, "NSA Surveillance Program Failed to Invade Tamerlan Tsarnaev's Privacy," The Daily Beast, July 12, 2013, http://www.thedailybeast.com/articles/2013/06/12/nsa-surveillance-program-failed-to-invade-tamerlan-tsarnaev-s-privacy.html.

[75] Senator Mark Udall, critic of the surveillance practices has asked the DNI to provide concrete examples, but nothing has come forth so far. *See* http://www.markudall.senate.gov/?p=press_release&id=3542

[76] Karl Rove, "Did Holder mislead Congress about targeting reporters like James Rosen?," Fox News, May 23, 2013, http://www.foxnews.com/opinion/2013/05/24/did-holder-mislead-congress-about-targeting-reporters-like-james-rosen/.

[77] Glenn Greenwald, "Glenn Greenwald: detaining my partner was a failed attempt at intimidation," The Guardian, August 19, 2013, http://www.theguardian.com/commentisfree/2013/aug/18/david-miranda-detained-uk-nsa.

Constitutional were influenced by the flaws and strengths of the English government. The Constitution of the United States created a government of checks and balances between the judicial, executive, and legislative branches. In the Federalist Papers No. 51, James Madison wrote that each department of government should "be the means of keeping each other in their proper places."[78] As such, each branch provides a viable outlet for correcting the problems with FISA.

The concept of Parliamentary sovereignty and the legislature's relationship with other parts of government is a unique feature of British history that has developed over the last eight-hundred years. The supreme authority of Parliament over the monarchy was gradually established, starting with the Magna Carta in 1215 and culminating in the Glorious Revolution of the later 17th century. Naturally, the main source of redress will be Parliament. However, there is an additional component when discussing redress in the United Kingdom in the form of the European Union. European Union treaties, in conjunction with domestic law, could provide Britons an opportunity to enact change via domestic and European courts.

C. Judicial Remedies and Key Differences in the United States and United Kingdom judicial systems

The Supreme Court of the United States has been the principle branch for the articulation and protection of the right of privacy in the American system of governance. The Supreme Court has been able to do so because of its most powerful check on the legislative and executive branches: judicial review. Much like the right to privacy, the power of judicial review is not explicitly stated in the Constitution of the United States. In *Marbury v. Madison*, Chief Justice Marshall interpreted Article III and Article IV, the clauses establishing the judicial branch and

---

[78] *See* http://www.constitution.org/fed/federa51.htm

the Supremacy Clause respectively, to imply the power of judicial review. Without such a power, Chief Justice Marshall noted, a law could be both contrary to the constitution yet valid at the same time, which "would subvert the very foundation of all written Constitutions."[79]

Due to the power of judicial review, it is possible for one to challenge the FAA, which has been used as the pretext for the NSA's PRISM program. Challenges to government spying programs have been brought and reviewed by the Supreme Court as shown in *United States v. United States Dist. Court.* However, establishing such a claim is not an easy task.

In 2007, the ACLU brought suit against the Bush administration in *American Civil Liberties Union v. National Security Agency.*[80] The complaint alleged that the Terrorist Surveillance Program, a forerunner of sorts to current NSA practices, violated the plaintiff's rights under a variety of theories including under the First Amendment, Fourth Amendment, and the FISA Act. The Court held that the claim should be dismissed because of standing issues. The Court stated that the plaintiffs failed to "produce any evidence that any of their own communications have ever been intercepted by the NSA" or that any injury had occurred in the form of "criminal prosecution, deportation, administrative inquiry, civil litigation, or even public exposure."[81]

The evidentiary problem is *American Civil Liberties Union v. National Security Agency* is the first hurdle that a potential plaintiff must pass. The NSA argued that the State Secrets Doctrine allows the government to "bar the discovery or admission of evidence that would 'expose [confidential] matters which, in the interest of national security, should not be divulged.'"[82] The fact that the plaintiffs in *ACLU v. NSA* could not establish an evidentiary basis

---

[79] Marbury v. Madison, 5 U.S. 137, 178 (1803).
[80] This case challenged §702(a)
[81] *ACLU v. NSA*,493 F.3d 644, 653 (6th Cir. 2007)
[82] *Id.* at 650 *citing United States v. Reynolds*, 345 U.S. 1, 10 (1953).

does separate it from *United States v. United States Dist. Court.*, in which the plaintiff were able to show that the government indeed was illegally tapping there phones.

A second barrier that a potential plaintiff would need to surpass is showing an injury. In order to bring a claim, an injury must be shown to be "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."[83] In *ACLU v. NSA*, the Sixth Circuit was skeptical of the First Amendment injuries, such as not being able to communicate freely with their journalistic sources. Again, this case can be contrasted with *United States v. United States Dist. Court.*, in which the injury of incarceration was apparent.

The problems of judiciability were again highlighted in *Clapper v. Amnesty Int'l USA*. The plaintiffs, who were lawyers, journalists and human rights workers, claimed that FAA §702(a) "compromises their ability to locate witnesses, cultivate sources, obtain information, and communicate confidential information to their clients."[84] The Supreme Court held that their claim failed because "it is speculative whether the Government will imminently target communications to which respondents are parties," failing the injury prong.[85]

An underlying theme is present in *Clapper v. Amnesty Int'l USA*, and to a lesser extent in *ACLU v. NSA*, is a trust in the protective framework of FISA which makes the potential for injury less likely. In the majority opinion of *Clapper,* Justice Thomas stated that "Congress created a comprehensive scheme in which the [FISC] evaluates the Government's certifications,

---

[83] *Clapper v. Amnesty Int'l USA*,133 S. Ct. 1138, 1147 (2013) *citing Monsanto Co. v. Geertson Seed Farms,* 130 S. Ct. 2743, 2752 (2010)
[84] *Id.* at 1145 (2013).
[85] *Id.* at 1148.

targeting procedures, and minimization procedures--including assessing whether the targeting and minimization procedures comport with the Fourth Amendment."[86]

Conversely, the four-person dissent written by Justice Breyer saw the case much differently. Justice Breyer saw the injury in more concrete terms, noting that the injury alleged "is as likely to take place as are most future events that commonsense inference and ordinary knowledge of human nature tell us will happen," pointing to past behavior and capabilities of the NSA.[87] Further, Justice Breyer also interpreted the concept of injury in a less restrictive way as "something more akin to 'reasonable probability' or 'high probability.'"[88]

More recently, a D.C. Circuit case, *Klayman v. Obama*, has breathed hope into a successful challenge against the FAA. The plaintiffs sought an injunction to bar the collection of their data and to destroy any data previously collected under provision of the PATRIOT Act and FAA §702.[89] The Court held that the plaintiffs alleged a sufficient injury for two reasons. First, the Court took a view of injury in the mold of Justice Breyer in *Clapper*. Second, the Court was directly influenced by the Snowden leaks. The Court wrote that:

> "The Supreme Court decided Clapper just months before the June 2013 news reports revealed the existence and scope of certain NSA surveillance activities. Thus, whereas the plaintiffs in Clapper could only speculate as to whether they would be surveilled at all, plaintiffs in this case can point to strong evidence that, as Verizon customers, their telephony metadata has been collected for the last seven years (and stored for the last five) and will continue to be collected barring judicial or legislative intervention...In addition, the Government has declassified and authenticated an April 25, 2013 FISC Order signed by Judge Vinson, which confirms that the NSA has indeed collected telephony metadata from Verizon."[90]

---

[86] *Id.* at 1154.
[87] *Id.* at 1155.
[88] *Id.* at 1165.
[89] *Klayman v. Obama*, 957 F. Supp. 2d 1, 8 (D.D.C.2013). When ruling on a motion for preliminary injunction, a court must consider "whether (1) the plaintiff has a substantial likelihood of success on the merits; (2) the plaintiff would suffer irreparable injury were an injunction not granted; (3) an injunction would substantially injure other interested parties; and (4) the grant of an injunction would further the public interest." *citing* Sottera, Inc. v. Food & Drug Admin., 627 F.3d 891, 893 (D.C. Cir. 2010)
[90] *Id.* at 26.

In order to grant the injunction, the Court also had to make a determination on the likelihood of the plaintiff's Fourth Amendment claims. The collection of data was held to be a search because a person's reasonable expectation of privacy was "violated when the Government, without any basis whatsoever to suspect them of any wrongdoing, collects and stores for five years their telephony metadata for purposes of subjecting it to high-tech querying and analysis without any case-by-case judicial approval."[91] In addition, the Court held that the challenge would likely be successful because the plaintiffs have shown that "their privacy interests outweigh the Government's interest in collecting and analyzing bulk telephony metadata," particularly because the government failed to "cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature."[92]

The D.C. District Court granted the injunction but stayed its implementation pending appeal. While *Klayman* should give privacy advocates reason to be slightly more optimistic, judicial finality on the FAA and NSA programs will need Supreme Court approval. When or if this approval will come is questionable, and in the meantime the average citizens' data will continue to be collected.

Although recent case law in the United States indicates that a favorable challenge to the FAA could be successful, a judicial remedy under British law will be much harder. Domestic judicial review in the American mold is impossible under the British model. However, a declaration of incompatibility or a challenge in the European Court of Human Rights could prove fruitful.

---

[91] *Id.* at 37.
[92] *Id.* at 40.

It is often said that Britain has an unwritten constitution, but this is not entirely true. Under the concept of Parliamentary sovereignty, Acts of Parliament are the supreme law of the land. This means that in effect, the Regulation of Investigatory Powers Act *is part* of the constitution of Britain, making domestic judicial review illogical.

Although an Act of Parliament cannot be struck down under the Human Rights Act, a declaration of incompatibility is not as hollow as it might first appear. As of April 2013, twenty-eight declarations of incompatibility have been made in a variety of areas including familial and reproductive rights, prisoners' rights, and sovereign immunity.[93] Of these twenty eight, twenty have resulted in the law being modified while eight have been overturned on appeal.[94]

The Human Rights Act, in conjunction with Article 8 of European Convention on Human Rights, has had some domestic success in the civil realm of privacy. In *Campbell v Mirror Group Newspapers Ltd*, the defendant, a popular tabloid newspaper, had taken and published pictures of Naomi Campbell, a famous model, leaving a rehabilitation clinic.[95] The House of Lords, split three to two, held in favor of Ms. Campbell and her breach of privacy claim. More importantly, all five members of the House of Lords acknowledged that Article 8 created a right to privacy that had to be balanced proportionally on a case-by-case basis with the freedom of expression guaranteed by Article 10.[96] Whether the judiciary would use Article 8 to declare part of RIPA incompatible is questionable, but the existence of such legal framework, at least in the civil context, is an important first step.

---

[93] Taken from the London School of Economics and Political Science. For complete information, *see* http://www.lse.ac.uk/humanRights/documents/2013/incompatibilityHRA.pdf
[94] *Id.*
[95] *Campbell v Mirror Group Newspapers Ltd.*, [2004] UKHL 22
[96] *Id.*

Civil liberties groups in Britain have filed a case against the government in the European Court of Human Rights. In *Big Brother Watch and others v. The United Kingdom*, the plaintiffs assert two different claims against the government. The first claim is that the receiving of data on British citizens from the United States is violates Article 8 of the ECHR.[97] The second asserts that the "interception, search, analysis, dissemination, storage and destruction of data relating to 'external' communications" under RIPA 8(4) also violates Article 8 of the ECHR.[98]

The European Court of Human Rights can only hear cases under certain circumstances. First, the plaintiff must claim to be victims of a violation under Article 8. This prong is similar to the injury requirement in the United States, but the bar it set much lower than the approach taken by Justice Breyer in *Clapper*. The first prong should be easy to overcome since the European Court of Human Rights has held multiple times that the existence of spying programs alone is enough to constitute a violation of privacy under Article 8.[99] Second, the European Court of Human Rights must find that the plaintiffs have exhausted all domestic remedies. The European Court of Human Rights held in *Kennedy v. UK* that the Investigatory Powers Tribunal, where RIPA says all complaints should be directed, cannot provide an effective judicial remedy of incompatibility, thereby avoiding the problem of non-exhaustion.[100]

As opposed to declaring whether the law violate the constitution, the European Court of Human Rights will have to decide whether or not RIPA is "'in accordance with the law' and 'necessary in a democratic society' within the meaning of Article 8 of the

---

[97] *Big Brother Watch and others v. The United Kingdom*, No. 58170/13 http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-140713#{"itemid":["001-140713"]}
[98] *Id.*
[99] *Iordachi and others v. Moldova,* No. 25198/02, § 34, ECHR 2009
[100] *Kennedy v. the United Kingdom,* No. 26839/05, § 109-112, ECHR 2010

Convention."[101] This means that European Court of Human Rights will effectively be conducting a proportionality test. The obvious justification for the law is national security, which the Court will find acceptable on its face. However, this interest will have to be proportional to its goals based on a variety of factors including the scope of the law, clarity of procedures, and the viability of safeguards.

D. Legislative Remedies

The process to repeal or alter the FISA Amendments Act of 2008 and Regulation of Investigatory Powers Act 2000 is a fairly straightforward in theory. However, whether the political will or desire of each nation's legislative body exists to change the law is doubtful. In addition, although both pieces of legislation have certain provisions that make the NSA and GCHQ accountable for their practices, they have no effect.

In the United States, the FAA was passed by Congress by a margin of 69 to 28 with three not voting. The effort was bipartisan, but all twenty eight nays were Democrats.[102] The amendments were extended for another five year on December 28, 2012, this time by a larger margin of 73 to 23 with 4 not voting. Again, almost all the no-votes were cast by Democrats, with three Republicans, Mike Lee (UT), Rand Paul (KY), and Lisa Murkowski (AK) voting no as well.[103] In the House of Representatives, both votes were overwhelmingly bipartisan.

When news of the PRISM program broke, the majority of the Senate tended to be in favor the NSA's practices while condemning Snowden. Dianne Feinstein, the Democratic chairwoman of the Senate Intelligence Committee, stated that PRISM was within the law and

---

[101] *Big Brother Watch and others v. The United Kingdom*, No. 58170/13

[102] *See* http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=110&session=2&vote=00168#position

[103] *See* http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=112&session=2&vote=00236#position

necessary to keep the country safe.[104] Others, such as John McCain and Mark Udall, opined that the law was necessary but should be re-examined.[105] Senator Rand Paul condemned the program and believed that a lawsuit should be filed against the NSA.[106]

It seems as though Congress will next address the issue when the FAA requires reauthorization in 2017. Unsurprisingly, whatever position various politicians have publically stated, no real efforts have been taken by either party to correct the FAA. President Obama has stated repeatedly that he believes the programs are within the boundaries of the Constitution, so any encouragement by the White House is unlikely.

Under the FAA, the Attorney General is required every six months to inform the House and Senate Intelligence Committees of certain activities. Reports include certifications of targeting and minimization procedures as well as the number of orders granted, modified, or denied.[107] These provisions seem to have zero effect on the members of the committees and do not really provide any meaningful oversight.

In the United Kingdom, Members of Parliament reacted harshly towards Edward Snowden. Prime Minister David Cameron stated that protective measures were in place and that the program was keeping the nation safe.[108] Many other MP's, including Deputy Prime Minister Nick Clegg, stated in broad, general terms that the leaks were extremely damaging to national security.[109]

---

[104] Caren Bohan, "Lawmakers urge review of domestic spying, Patriot Act," Chicago Tribune, June 9, 2013, http://articles.chicagotribune.com/2013-06-09/news/sns-rt-us-usa-security-lawmakersbre9580ab-20130609_1_guardian-national-security-agency-surveillance.
[105] Id.
[106] Id.
[107] 50 U.S.C §1881f
[108] Paul Cooper, "David Cameron: 'GCHQ snooping keeps us safe.'" ITProPortal. Last modified October 13, 2013. http://www.itproportal.com/2013/10/08/david-cameron-gchq-snooping-keeps-us-safe/.
[109] Rob Williams, "Snowden leaks published by the Guardian were damaging to security, says Nick Clegg," The Telegraph, October 10, 2013, http://www.independent.co.uk/news/uk/politics/snowden-leaks-published-by-the-guardian-were-damaging-to-security-says-nick-clegg-8871894.html.

The British Parliament has taken a much more active role in reviewing the GCHQ and the Tempora program because of RIPA's framework. RIPA established the Investigatory Powers Tribunal, or IPT, which has the power to consider complaints about the surveillance practices of certain spy agencies, including the GCHQ.[110] According to the IPT, its purpose is to "ensure that public authorities act in ways that are compatible with the Human Rights Act 1998" and to provide "a right of redress for anyone who believes they have been a victim of unlawful action under RIPA or wider human rights infringements."[111]

However, any sort of redress from the IPT seems to be a futile endeavor. The IPT, by its own admission, has stated that in "no case so far brought to the Tribunal has one of the intelligence agencies been found to have acted unlawfully."[112] Human right groups such as Privacy International, Liberty, and Amnesty International have lodged complaints with the IPT over GCHQ's practices. The success of these still-pending complaints remains uncertain.[113]

Part VI: Conclusion

The United States of America and the United Kingdom of Great Britain have greatly expanded their electronic surveillance programs to combat the growth of international terrorism after the September 11th attacks. In the United States, the Foreign Intelligence Surveillance Amendments Act of 2008 altered the original 1978 act in significant ways. The Amendments broadened who could be targeted without a warrant by expanding the warrantless power to all persons reasonably believed to be foreign citizens. Similarly, the United Kingdom's Regulation of Investigatory Powers Act allowed the Government Communications Headquarters to collect data on all communications originating and terminating outside Great Britain. Until June 2013,

---

[110] Regulation of Investigatory Powers Act, 2000, c. 23, § 65
[111] *See* http://www.ipt-uk.com/section.aspx?pageid=1
[112] *See* http://www.ipt-uk.com/section.aspx?pageid=5
[113] James Ball, "GCHQ views data without a warrant, government admits," The Guardian, October 28, 2014, http://www.theguardian.com/uk-news/2014/oct/29/gchq-nsa-data-surveillance.

the public remained largely unaware how extensive electronic surveillance was. This all changed when documents released by Edward Snowden showed that the surveillance programs run by the NSA and GCHQ, codenamed PRISM and Tempora respectively, had been collecting data on domestic citizens, exceeding their statutory scope and likely violating the right to privacy guaranteed by each nation's constitution.

The unique framework of the United States and Great Britain's constitutions allows for different forms of redress. The Constitution of the United States creates a system of checks and balances in which citizens can petition for change through Congress and the Supreme Court. The power of judicial review in United States provides an avenue for redress that is unavailable domestically in the British form of government. Despite the availability of domestic judicial review, the chances of successful judicial redress are questionable. In order to bring suit in the federal courts, one must show injury under the doctrine of standing. In *ACLU v. NSA* and *Clapper v. Amnesty Int'l*, the Supreme Court dismissed the cases because the plaintiff's proposed First Amendment injuries were not concrete enough to meet the standing requirement. However, there are some encouraging signs that the Supreme Court could rule favorably for future plaintiffs. In *Klayman v. Obama*, the D.C. District Court, influenced by the Snowden leaks, held that the First Amendment injuries were enough to establish standing. In addition, the Court held that the government's national security interests were outweighed by the plaintiff's privacy rights.

In the United Kingdom, the judiciary does not have the power to overturn Acts of Parliament because of the principle of Parliamentary Supremacy, which holds that Acts of Parliament are the supreme law of the land. However, the potential for review via the European Court of Human Rights does provide a separate level of judicial overview. The

European Court of Human Rights has a lower bar for standing that only require a violation of European law and an exhaustion of all domestic remedies. The European Court of Human Rights has already held that the mere existence of spying programs can be a violation of one's right and that the legislative remedies provided by RIPA are not an adequate remedy.

The legislatures of the United States and the United Kingdom could easily alter the FISA and RIPA framework, but this seems highly unlikely. In the United States, few senators have expressed any interest of changing the FISA framework. Britain's Investigatory Powers Tribunal is specifically charged with reviewing citizen complaints and the general practices of the GCHQ, but has never found any of the GCHQ's practices to be illegal.

There is one final factor that bares discussion: the people. When Edward Snowden decided to reveal the practices of the NSA and GCHQ, he stated that he did so to prompt a discussion among the people over privacy rights and electronic surveillance to reform the system. The goal of a public debate was accomplished, for a few months at least. Although court cases are pending in the United States and Great Britain, no real change has occurred in the year and a half following the disclosures.

It is appropriate to ask why there have been no changes despite what clearly seems to be ongoing violations of people's constitutionally guaranteed privacy rights. Polls indicate that although the public is not entirely comfortable with electronic surveillance, there is a legitimate fear of terrorism and a rather large degree of deference to national security concerns. In polls conducted by the Pew Research Center, 49% of Americans said the leaks served the public interest, while 44% thought they did harm.

Among young people under thirty, who are more internet savvy, 57% thought Snowden served a public interest and only 35% said the leaks were harmful. On the other hand, 53% of Americans believed that the programs used by the NSA helped stop terrorist attacks, despite the lack of evidence. When asked about government spying that targeted them specifically, 63% said they feel their rights would be violated if their data was collected.[114]

In Britain, polls conducted by YouGov actually skewed towards approval for government spying. Only 35% of people thought the disclosures were good thing as opposed to the 43% believed the leaks were harmful. However, 46% said agencies should not be allowed to store metadata, while 38% said they should be allowed. When asked if government agencies had too much power when conducting surveillance on its citizen, 19% said too much, 22% said not enough, and a solid 42% minority said the balance was right.[115]

The aforementioned poll results may help explain the lack action and have a direct effect on the potential for redress. Public interest groups like the ACLU and Big Brother Watch have taken up the mantle of defending privacy rights in the judicial system on behalf of ordinary people. However, *Klayman* and *Big Brother Watch* may fail, leaving the legislature as the last avenue for reform. If the notion of Congress and Parliament being the voice of people is true, it seems very likely that what appears to be unconstitutional behavior will continue by the NSA and GCHQ. It was once said by

---

[114] The poll results in this paragraph were taken from: "Public Split over Impact of NSA Leak, But Most Want Snowden Prosecuted." Pew Research Center for the People & Press. Last modified June 17, 2013. http://www.people-press.org/2013/06/17/public-split-over-impact-of-nsa-leak-but-most-want-snowden-prosecuted/.

[115] The poll results in this paragraph were taken from: Will Dahlgreen, "Little appetite for scaling back surveillance," YouGov, last modified October 13, 2013, https://yougov.co.uk/news/2013/10/13/little-appetite-scaling-back-surveillance/.

Savoyard philosopher Joseph-Marie de Maistre that "every nation gets the government it deserves." De Maistre's words may prove prophetic in the case of government surveillance. The debate that Edward Snowden wanted people around the world to have happened; it is a shame for Edward Snowden that the people may have chosen a different side.

Works Cited

Ackerman, Spencer, and James Ball. "Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ." The Guardian, February 28, 2014. http://www.theguardian.com /world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.

Ball, James. "GCHQ views data without a warrant, government admits." The Guardian, October 28, 2014. http://www.theguardian.com/uk-news/2014/oct/29/gchq-nsa-data-surveillance.

Bohan, Caren. "Lawmakers urge review of domestic spying, Patriot Act." Chicago Tribune, June 9, 2013. http://articles.chicagotribune.com/2013-06-09/news/sns-rt-us-usa-security-lawmakersbre9580ab-20130609_1_guardian-national-security-agency-surveillance.

Cooper, Paul, "David Cameron: 'GCHQ snooping keeps us safe.'" ITProPortal. Last modified October 13, 2013. http://www.itproportal.com/2013/10/08/david-cameron-gchq-snooping-keeps-us-safe/.

Dahlgreen, Will. "Little appetite for scaling back surveillance." YouGov. October 13, 2013. https://yougov.co.uk/news/2013/10/13/little-appetite-scaling-back-surveillance/.

Daly, Michael. "NSA Surveillance Program Failed to Invade Tamerlan Tsarnaev's Privacy." The Daily Beast, July 12, 2013. http://www.thedailybeast.com/articles/2013/06/12/nsa-surveillance-program-failed-to-invade-tamerlan-tsarnaev-s-privacy.html.

Drum, Kevin. "Washington Post Provides New History of NSA Surveillance Programs." Mother Jones, July 15, 2013. http://www.motherjones.com/kevin-drum/2013/06/washington-post-provides-new-history-nsa-surveillance-programs.

Gellman, Barton, and Ashkan Soltani. "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say." The Washington Post, October 30, 2013. http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

Greenwald, Glenn. No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. New York: Metropolitan Books, 2014.

"XKeyscore: NSA tool collects 'nearly everything a user does on the internet.'" The Guardian, July 31, 2013. http://www.theguardian.com/world/2013/jul/31/ nsa-top-secret-program-online-data.

"Glenn Greenwald: detaining my partner was a failed attempt at intimidation." August 19, 2013. http://www.theguardian.com/commentisfree/2013/aug/18/david-miranda-detained-uk-nsa.

Greenwald, Glenn, and Ewen MacAskill. "NSA Prism program taps in to user data of Apple, Google and others." The Guardian, June 7, 2013.http://www.theguardian.com/ world/2013/jun/06/ us-tech-giants-nsa-data.

Greenwald, Glenn, Ewen MacAskill, and Laura Poitras. "Edward Snowden: the whistleblower behind the NSA surveillance revelations." The Guardian, June 11, 2013. http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies, and James Ball. "GCHQ taps fibre-optic cables for secret access to world's communications." The Guardian, June 21, 2013. http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

Pilkington, Ed. "Declassified NSA files show agency spied on Muhammad Ali and MLK." The Guardian, September 26, 2013. http://www.theguardian.com/world/2013/sep/26/nsa-surveillance-anti-vietnam-muhammad-ali-mlk.

"Public Split over Impact of NSA Leak, But Most Want Snowden Prosecuted." Pew Research Center for the People & Press. Last modified June 17, 2013. http://www.people-press.org/2013/06/17/public-split-over-impact-of-nsa-leak-but-most-want-snowden-prosecuted/.

Roberts, Dan, Spencer Ackerman, and Tania Branigan. "Clapper admits secret NSA surveillance program to access user data." The Guardian, June 7, 2013. http://www.theguardian.com/world/2013/jun/07/clapper-secret-nsa-surveillance-prism.

Rove, Karl. "Did Holder mislead Congress about targeting reporters like James Rosen?" Fox News, May 23, 2013. http://www.foxnews.com/opinion/2013/05/24/did-holder-mislead-congress-about-targeting-reporters-like-james-rosen/.

Timberg, Craig, and Barton Gellman. "NSA paying U.S. companies for access to communications networks." The Washington Post, August 21, 2013. http://www.washingtonpost.com/world/ national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html.

Williams, Rob. "Snowden leaks published by the Guardian were damaging to security, says Nick Clegg." The Telegraph, October 10, 2013. http://www.independent.co.uk/news/uk/ politics/snowden-leaks-published-by-the-guardian-were-damaging-to-security-says-nick-clegg-8871894.html.